Exhibit 18

Excerpts of SW-SEC00313350

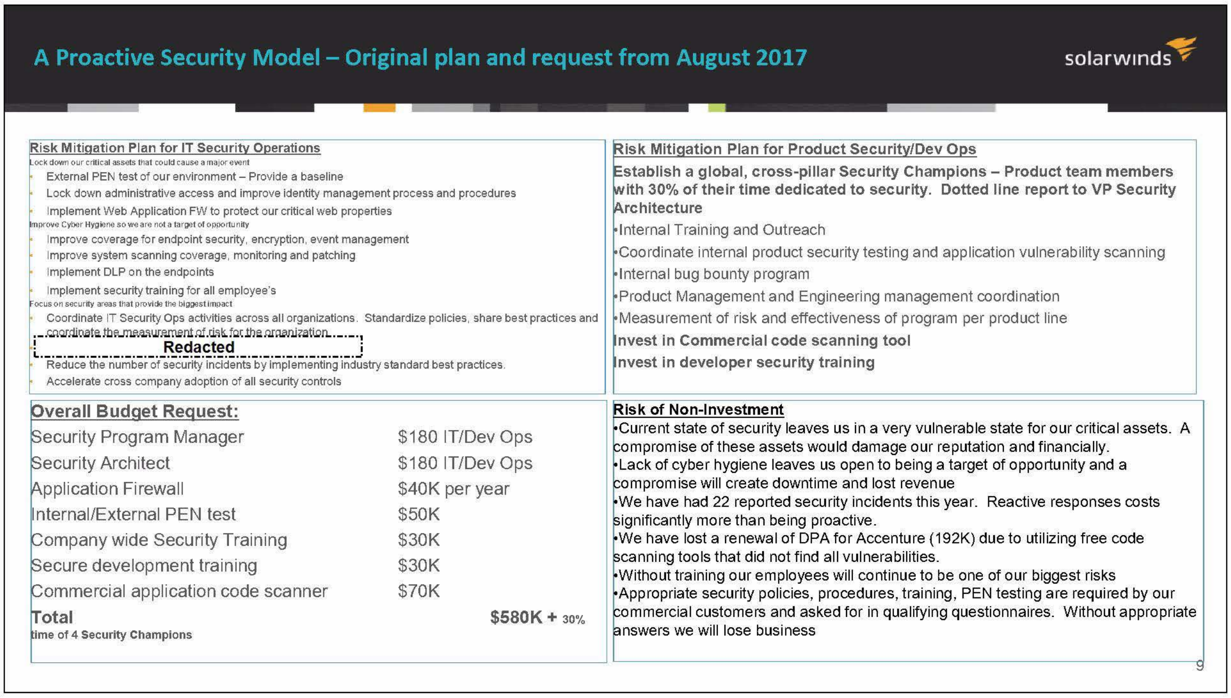
From: Brown, Timothy [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=A1BCD95116E84D6692DD89F9D55C5B7A-BROWN, TIMO]
Sent: 10/29/2018 9:14:30 PM
To: Johnson, Rani [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=0ee57945f15e47b3abaa99a59170ad3f-Johnson, Ra]
Subject: Solarwinds state of security operations [Autosaved].pptx
Attachments: Solarwinds state of security operations [Autosaved].pptx

This powerpoint contains the current state of security slides updated for October. A review of what we asked for last August and a red yellow green status showing how we have done on our initiatives. A 2019 plan and ask for security. We can review in tomorrow but it's a reasonable place to start.

Tim

INFORMATION SECURITY -

Risk review October 2018



A Proactive Security Model – Original plan and request from August 2017

solarwinds

Risk Mitigation Plan for IT Security Operations

Lock down our critical assets that could cause a major event

- External PEN test of our environment – Provide a baseline
- Lock down administrative access and improve identity management process and procedures
- Implement Web Application FW to protect our critical web properties

Improve Cyber Hygiene so we are not a target of opportunity

- Improve coverage for endpoint security, encryption, event management
- Improve system scanning coverage, monitoring and patching
- Implement DLP on the endpoints
- Implement security training for all employee's

Focus on security areas that provide the biggest impact

- Coordinate IT Security Ops activities across all organizations. Standardize policies, share best practices and coordinate the measurement of risk for the organization.
- Redacted
- Reduce the number of security incidents by implementing industry standard best practices.
- Accelerate cross company adoption of all security controls

Risk Mitigation Plan for Product Security/Dev Ops

Establish a global, cross-pillar Security Champions – Product team members with 30% of their time dedicated to security. Dotted line report to VP Security Architecture

- Internal Training and Outreach
- Coordinate internal product security testing and application vulnerability scanning
- Internal bug bounty program
- Product Management and Engineering management coordination
- Measurement of risk and effectiveness of program per product line

Invest in Commercial code scanning tool

Invest in developer security training

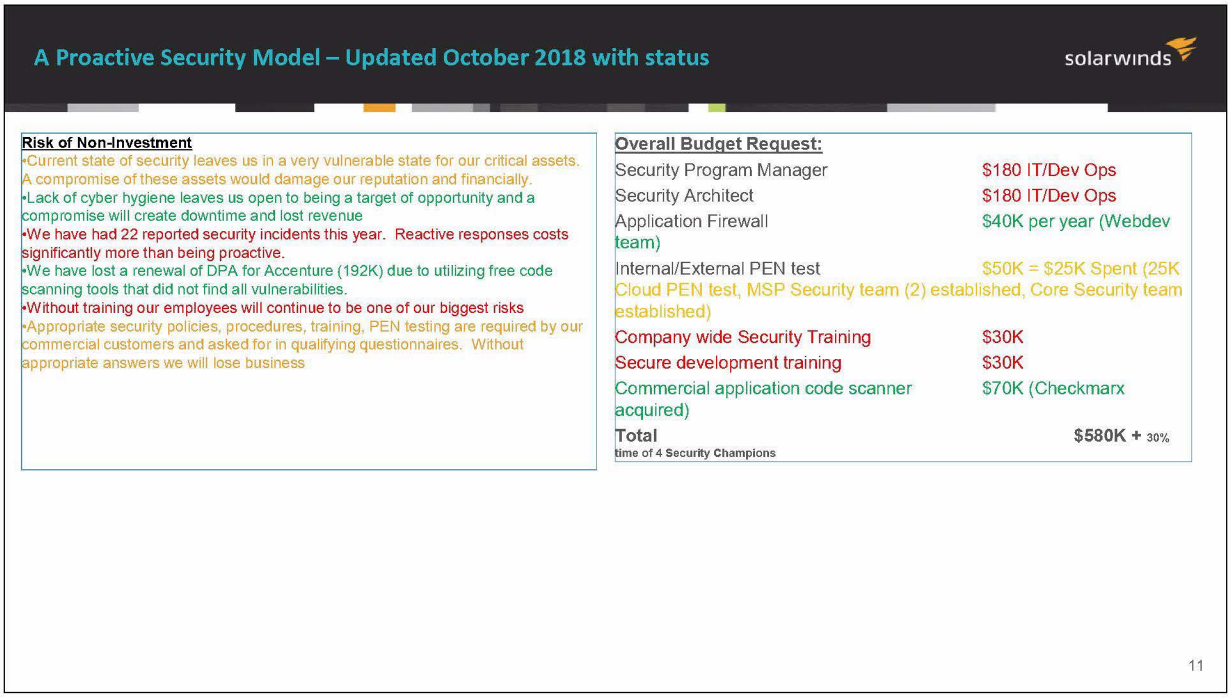
Overall Budget Request:

Security Program Manager	$180 IT/Dev Ops
Security Architect	$180 IT/Dev Ops
Application Firewall	$40K per year
Internal/External PEN test	$50K
Company wide Security Training	$30K
Secure development training	$30K
Commercial application code scanner	$70K
Total	**$580K +** 30%

time of 4 Security Champions

Risk of Non-Investment

- Current state of security leaves us in a very vulnerable state for our critical assets. A compromise of these assets would damage our reputation and financially.
- Lack of cyber hygiene leaves us open to being a target of opportunity and a compromise will create downtime and lost revenue
- We have had 22 reported security incidents this year. Reactive responses costs significantly more than being proactive.
- We have lost a renewal of DPA for Accenture (192K) due to utilizing free code scanning tools that did not find all vulnerabilities.
- Without training our employees will continue to be one of our biggest risks
- Appropriate security policies, procedures, training, PEN testing are required by our commercial customers and asked for in qualifying questionnaires. Without appropriate answers we will lose business



A Proactive Security Model – Updated October 2018 with status

solarwinds

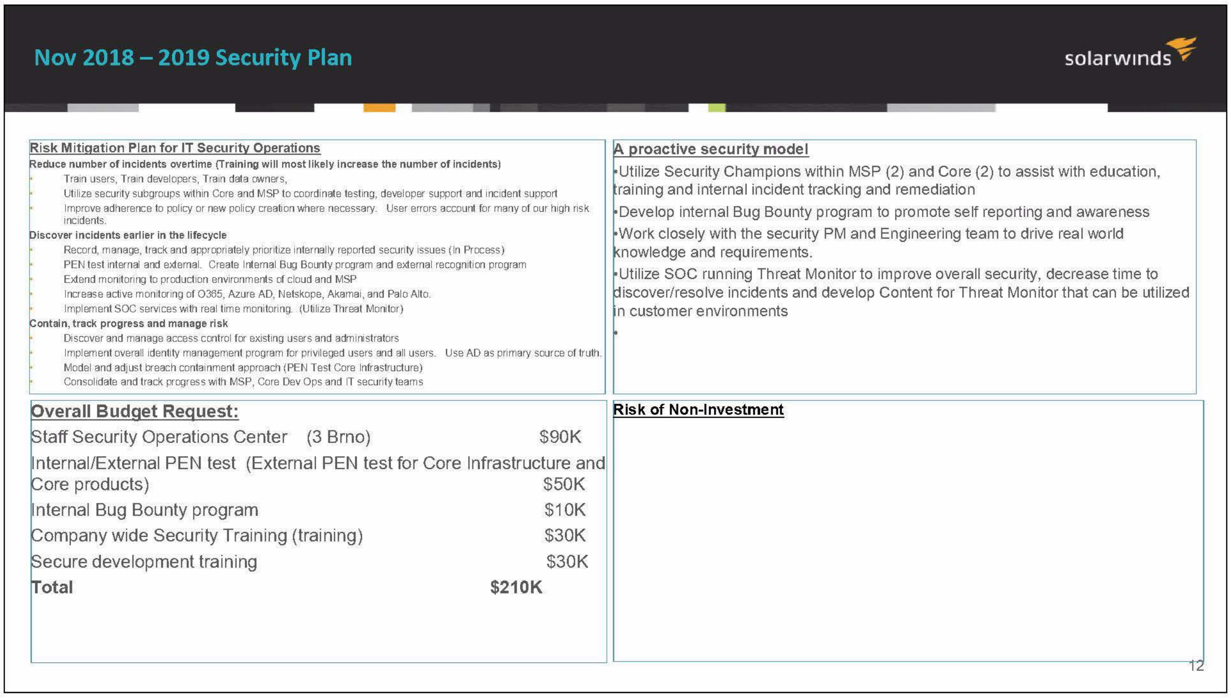
Risk of Non-Investment

- Current state of security leaves us in a very vulnerable state for our critical assets. A compromise of these assets would damage our reputation and financially.
- Lack of cyber hygiene leaves us open to being a target of opportunity and a compromise will create downtime and lost revenue
- We have had 22 reported security incidents this year. Reactive responses costs significantly more than being proactive.
- We have lost a renewal of DPA for Accenture (192K) due to utilizing free code scanning tools that did not find all vulnerabilities.
- Without training our employees will continue to be one of our biggest risks
- Appropriate security policies, procedures, training, PEN testing are required by our commercial customers and asked for in qualifying questionnaires. Without appropriate answers we will lose business

Overall Budget Request:

Security Program Manager	$180 IT/Dev Ops
Security Architect	$180 IT/Dev Ops
Application Firewall	$40K per year (Webdev team)
Internal/External PEN test	$50K = $25K Spent (25K Cloud PEN test, MSP Security team (2) established, Core Security team established)
Company wide Security Training	$30K
Secure development training	$30K
Commercial application code scanner	$70K (Checkmarx acquired)
Total	**$580K + 30%**

time of 4 Security Champions



Nov 2018 – 2019 Security Plan

solarwinds

Risk Mitigation Plan for IT Security Operations

Reduce number of incidents overtime (Training will most likely increase the number of incidents)

- Train users, Train developers, Train data owners,
- Utilize security subgroups within Core and MSP to coordinate testing, developer support and incident support
- Improve adherence to policy or new policy creation where necessary. User errors account for many of our high risk incidents.

Discover incidents earlier in the lifecycle

- Record, manage, track and appropriately prioritize internally reported security issues (In Process)
- PEN test internal and external. Create Internal Bug Bounty program and external recognition program
- Extend monitoring to production environments of cloud and MSP
- Increase active monitoring of O365, Azure AD, Netskope, Akamai, and Palo Alto.
- Implement SOC services with real time monitoring. (Utilize Threat Monitor)

Contain, track progress and manage risk

- Discover and manage access control for existing users and administrators
- Implement overall identity management program for privileged users and all users. Use AD as primary source of truth.
- Model and adjust breach containment approach (PEN Test Core Infrastructure)
- Consolidate and track progress with MSP, Core Dev Ops and IT security teams

A proactive security model

- Utilize Security Champions within MSP (2) and Core (2) to assist with education, training and internal incident tracking and remediation
- Develop internal Bug Bounty program to promote self reporting and awareness
- Work closely with the security PM and Engineering team to drive real world knowledge and requirements.
- Utilize SOC running Threat Monitor to improve overall security, decrease time to discover/resolve incidents and develop Content for Threat Monitor that can be utilized in customer environments
-

Overall Budget Request:

Staff Security Operations Center (3 Brno)	$90K
Internal/External PEN test (External PEN test for Core Infrastructure and Core products)	$50K
Internal Bug Bounty program	$10K
Company wide Security Training (training)	$30K
Secure development training	$30K
Total	**$210K**

Risk of Non-Investment